Remarks

In the Office action of July 13, 2007, claims 1-13 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite, on grounds that the term "approximate" used in the expression "approximate quotient q" throughout the several claims is a relative term. As stated on page 2 of the Office action (item 5): "The term 'approximate' is not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention."

However, in the present instance, the word "approximate" is not being used as a relative term at all, but merely as part of a convenient label "approximate quotient" for the value q. The term "approximate" itself does not serve to modify the value q in any real way, whether to define some degree of precision/uncertainty or otherwise affect a range of allowed values for q. Rather, the expression "approximate quotient" provides a label for the value q that keeps it separate from and avoids confusion with the other recited quotient value in the claims, namely the value q' labeled as a "randomized quotient", as well as the implied "true" quotient normally used in modular reduction operations of this kind of obtain the residue value. The value q itself in the present claims has a well-defined meaning as set forth, for example, in the specific way the computation unit estimates q in the second indented section of claim 1. (See also the equation recited in dependent claim 3.)

Because the term "approximate" more usually is used with a relative sense, the claims are herein amended (specifically claims 1, 3, 4, 6, 8, 11, and 12) to replace the label expression "approximate quotient" with an alternative label expression "estimated quotient value", and to refer to

"computing" an estimated quotient value q. The value q itself remains well-defined by the operational step recited in claims 1 and 8 for its computation. Thus, it should be clear that no relative terminology is intended, and the claims have a definite scope.

Claims 1-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Barrett's modular reduction method (described in the prior art documents cited on page 1, line 33 to page 2, line 12 of the application, as well as the documents mentioned in item 8 of the Office action) in view of Liardet et al. (U.S. Patent Application Publication No. 2003/0044014 A1).

Liardet et al. was cited for "teaching modifying an intermediary result with a random quantity, carrying out the calculation and restoring the expected result at the end of the modular reduction (paragraphs 0033-0035, 0041)." (O.A., item 10) The Office action asserts that "it would have been obvious to one of ordinary skill in the [art] at the time the invention was made to generate, in a random number generator, a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient $q' = q - E$, since Liardet states at paragraph 0031 that adding a random intermediate value to a calculation provides protection against attacks by differential power analysis."

Liardet et al. applies a random quantity r to an intermediary result $V2 = (V1 \cdot a) \bmod p$. The intermediary result and its randomized value V2', V2", V2'", etc. (depending on the embodiment) are equivalent to our number X to be reduced, not of our estimated quotient value q or its randomization q'. Liardet et al. does not teach randomizing of the quotient value that would be used in the modulo reduction operation itself, but only of the value that is subject to the reduction. Thus, in the example of Fig. 5, where an intermediary value V2 is modified by adding a random

multiple r of the modulus n, $V2' = V2 + r \cdot n$, the result B is recovered at a later step from V4' by a reduction modulo n, $B = V4' \bmod n$. Fig. 6 doesn't employ a modulo operation, but the intermediary result V2 is modified by adding a random value r, $V2'' = V2 + r$, then after a subsequent multiplication by a factor q, $V3'' + V2'' \cdot q$, the result B can be recovered from V4" by a subtraction of the product $(q \cdot r)$, $B = V4'' - q \cdot r$. Fig. 7 uses two different moduli p and n, so where an intermediary result is modified by a random value r under a first modulus p, $V2''' = (V1 \cdot a + r) \bmod p$, and subsequently operated upon, $V3''' = V2''' \cdot q$, so that the result V5 can be recovered by a subtraction of the product $(q \cdot r)$, $V5 = V4''' - q \cdot r$, prior to reduction by the second modulus n. The other embodiments (DSA-type) are basically similar, except that Fig. 8 randomly modifies the modulus q, $u2' = u1 + d \cdot t \bmod (q \cdot r)$, which necessitates a more complex recovery of the result $B = u3' = u2' \cdot k^{-1} \bmod q$. Nowhere does the quotient value q used in performing a modulo reduction get randomized. Thus, Liardet et al. does not suggest modifying Barrett's method in the manner claimed in the present application. Accordingly, claims 1-7 should be deemed patentable over the cited art. Dependent claims 2-7 also recite further limitations for which they also are patentable.

In particular, dependent claim 2 and 3 are further patentable because they differ from Barrett, with or without Liardet et al., in the manner of computing the estimated quotient value q. In the prior art method of Barrett, the precomputed recipient U of the modulus M is defined as $U = \lfloor b^{2n}/M \rfloor = \lfloor 2^{2nw}/M \rfloor$, whereas in claim 2 we use $U = \lfloor b^{2n+1}/M \rfloor = \lfloor 2^{2nw+w}/M \rfloor$, i.e., with an extra shift of one word. Likewise, in the prior art method of Barrett, the quotient q is computed using the stored value U as

$q = \lfloor \left(\lfloor X/b^{n-1} \rfloor \cdot U \right)/b^{n+1} \rfloor$, whereas in claim 3 we compute the estimated quotient value $q = \lfloor \left(\lfloor X/b^{n} \rfloor \cdot U \right)/b^{n+2} \rfloor$, i.e., with another extra shift of one word. By this difference, we ensure that the quotient value q is consistently underestimated, even before randomization. These extra word shifts are not taught or suggested by Barrett nor in any of the cited documents where Barrett's method is described. Thus, dependent claims 2 and 3 are patentable for their own reasons.

Claims 8-13 (computational hardware) were rejected under 35 U.S.C. § 103(a) as being unpatentable over Applicants' admitted prior art (page 3, line 23 - page 4, line 9) in view of Barrett's method and further in view of Liardet.

The cited operations sequencer comprising logic circuitry controls several stated operations of the computation unit in accord with program instructions so as to carry out a modular reduction, including "a randomization of said estimated quotient value with said random error value." As previously noted above, Liardet et al. does not disclose randomization of any quotient values, but only of the value to be reduced or the modulus. Accordingly, the subject matter set forth in claim 8 should likewise be patentable for the same reasons given above. Dependent claims 9-13 are patentable for the same reasons as claim 8, and further recite additional limitations for which they are also patentable.

In particular, claims 10 and 11 recite the same extra word shift that distinguishes the hardware computation of U and q from the prior Barrett computations, as discussed above for claims 2 and 3. The claimed hardware having a computation unit directed to perform the respective recited operations $U = \lfloor b^{2n+1}/M \rfloor$ and $q = \lfloor \left(\lfloor X/b^{n} \rfloor \cdot U \right)/b^{n+2} \rfloor$ is new and nonobvious, and thus claims 10 and 11 are deemed separately patentable.

ATM80:244.AMT

Further, in the Office action (items 25-33), claims 1-7 were provisionally rejected on the ground of nonstatutory (obviousness-type) double patenting over claims 1-6 of copending application no. 11/203,939. Claims 18-13 was provisionally rejected on the grounds of nonstatutory (obviousness-type) double patenting over claims 7-11 of copending application no 11/203,939. The copending application claims a modular reduction method and associated computational hardware that implements a new variation of Barrett's method that is applied instead to polynomial values in a binary finite field ($GF(2^n)$. A terminal disclaimer is submitted to overcome these provisional rejections.

Conclusion

Applicants request reconsideration of the claims in view of the amendments and remarks made herein. A Notice of Allowance is earnestly solicited.

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) on the date shown below.

Signed: Sally Azevedo
Typed Name: Sally Azevedo

Date: October 10, 2007

Respectfully submitted,

David M. Schneck
Reg. No. 43,094

Schneck & Schneck
P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733